REMARKS

Claims 1-24 are currently pending (claims 2, 3, 5 and 6 are presently withdrawn from consideration) in the subject application and are presently under consideration. Claims 1, 4, 7, 8, 11, 12, 14, 20, 21, 23 and 24 have been amended as shown on pages 2-7 of the Reply. These amendments do not introduce new matter and are fully supported by the specification as filed (*see* at least pg. 7, line 27 to pg. 8 line 6).

Applicants' representative thanks the Examiner for considering the remarks tendered by telephone on 26 February 2009 regarding amending the claims to include the use of substitute unpacking code in light of the presently withdrawn claims. It is believed that the highlighted distinctions will facilitate favorable prosecution of the pending application.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1 and 4 Under 35 U.S.C §112

Claims 1 and 4 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the enablement requirement. The claims have been amended to remove the term "entire" as requested by the Office. Although applicants' representative does *not* concede that this term was unsupported in the specification as originally filed, where the claim has been amended to comply with the Examiner's request, the argument is moot. As such, it is respectfully requested that the rejection of claims 1 and 4 under 35 U.S.C. § 112, first paragraph, be withdrawn.

II. Rejection of Claims 1, 4, and 7-24 Under 35 U.S.C. §103(a)

Claims 1, 4, and 7-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lucas et al. (US 6,968,261) in view of Thacker (US Pub. No. 2002/0035696) in further view of Edwards (US 6,968,461).

As previously stated, applicants' disclosed subject matter relates to detecting malware. The malware evaluator can intercept incoming code/data and searches for malicious code. This can be done by searching the arriving code/data for recognized patterns representative of known malicious code/data. Whereas hackers and the like have come to understand that these searches look for known patterns, the hackers have developed methods of packing malicious executable code to disguise it from traditional virus detecting software. By detecting and unpacking packed

code as it arrives, *e.g.*, intercepting it, the Applicants' invention can maintain the advantage over hackers' attempts at propagating malware through packed malicious executables. To facilitate this determination, a known unpacking code segment can be employed to unpack the packed code rather than employing the potentially malicious packer included with the received packed executable. This substitution of unpacker code can facilitate safer unpacking and analysis of packed executables to facilitate detection of malicious code therein.

Also as previously presented, the invention of Lucas generally relates to searching code for viruses in an "on-access antivirus system" (*see* Lucas, col. 3, line 47). Lucas describes that hackers have determined a particular weakness in anti-virus software that can cause the anti-virus software to "timeout" when system resources become severely taxed (*see* Lucas, col. 1, ln. 11-36). Lucas proposes a solution of decompressing compressed files from a hard drive device (Lucas, col. 3, ln. 51-52) on-access and scanning these decompressed files for viruses. In Lucas's proposal, malicious files that have been compressed, so as to bog down a system on decompression, can be parsed into smaller decompressed pieces to allow for sequential scanning of each decompressed piece for virus signatures by comparison to DATs (Lucas, col. 4, ln. 7-17). Lucas does not discuss intercepting code/data as it arrives at a computer. Further, Lucas does not disclose employing substitute unpacking code.

The Office's concedes that Lucas does not intercept incoming data (*see* Office Action at page 4). The Office turns to Thacker to support the absent code interception aspect of the Lucas malware protection system. Generally, Thacker describes intercepting code by using a virus trap (*e.g.*, an intermediary system in which the intercepted code can execute freely in an isolated environment). Under Thacker, code is allowed to proceed to the destination computer only after it is determined that the code is safe by "...selecting a by-pass for programs and attachments which are known to be good..." (*see* Thacker at [0013].) However, Thacker teaches away from the invention of the disclosed subject matter in that the invention of Thacker cannot be combined with Lucas in a manner that makes the subject invention obvious without altering the invention of Thacker as previously asserted. Further, Thacker is also silent in regard to employing substitute unpacking code facilitating detection of malware in that Thacker essentially lets the virus loose albeit in a quarantined environment. Applicants' representative maintains the prior arguments that Thacker and Lucas are incompatible, but reserves such argument where it is redundant wherein neither Lucas nor Thacker disclose employing substitute unpacker code.

Moreover, in light of the amendment to claims 1 and 4 as related to the term "entire", treatment of the additional Edwards reference is moot. However, it should be noted that Edwards is also silent with regard to employing a substitute unpacker to facilitate malware detection.

More specifically, independent claim 1 recites, "…at least one *substitute unpacker code segment, corresponding to a first unpacker code segment* of the first packed executable, such that an appropriate *substitute unpacker code segment is substituted for the first unpacker code segment* of the received first packed executable to facilitate *unpacking the first packed executable according to the substitute unpacker code rather than according to the first unpacker code*"(emphasis added), as part of the malware detection system. This aspect is not disclosed or suggested in Lucas, Thacker, or Edwards, either alone or in combination. As such, claim 1 is patentably distinct and is believed to be allowable over the cited art.

Similarly, the malware detection method of independent claim 4 recites, "accessing at least one *substitute unpacker code segment corresponding to a first incoming packed executable* of the incoming data…*substituting the substitute unpacker code segment for the first unpacker code segment* of the first packed executable…*generating a substitute unpacked executable employing the substitute unpacker code segment*…" (emphasis added). As asserted *supra*, none of Lucas, Thacker, or Edwards, either alone or in combination, disclose or suggest this aspect of the claimed subject matter. Therefore, claim 4 is also believed to be patentably distinct from the cited art and allowable as amended.

Additionally, claims 7-18 depend from independent claim 1 and claims 19-24 depend from independent claim 4. Wherein these claims depend from claims that are believed to be allowable, these dependant claims are also believed to be allowable. Therefore, based on the above remarks, the Applicants respectfully request that the Examiner withdraw the rejection of Claims 1, 4, and 7-24 under 35 USC § 103(a) as being obvious in view of Lucas in view of Thacker in further view of Edwards.

Moreover, claims 8 and 20 is believed to be separately allowable wherein claim 8 recites "wherein the employed substitute unpacker code is selected from a group of at least one modularized substitute unpacker modules" (claim 20 recites similar language), because each of Lucas, Thacker, and Edwards are silent with regard to employing substitute unpackers and therefore would necessarily be silent with regard to groups of modularized substitute unpacker

modules.

Further, claims 12 and 23 are similarly separately allowable wherein claim 12 recites "the corresponding generated substitute unpacked executable corresponding to a complete unpacked executable is unpacked *without executing any portion thereof*" (emphasis added, claim 23 recites similar language) wherein Thacker specifically teaches away from this aspect by stating that code is executed in a virus trap, *e.g.*, in an isolated environment before being allowed to the target computing device. As such, where Thacker teaches away from the claimed subject matter, the claimed subject matter is less obvious.

Additionally, wherein claim 15 recites, "first determining whether the incoming data is known malware before determining if the incoming data is a packed executable, and if not, then determining if the incoming data is a packed executable", said claim is believed to be separately allowable over the cited art. None of Lucas, Thacker, or Edwards, either alone or in combination, disclose or suggest systems that make determinations about the packed nature of received data after first checking for malware. More specifically, Lucas simply stands for segmental unpacking of received files to prevent memory overflow conditions that can be exploited by malicious code. As such, there is no discussion of first checking the code for malware before the segmented unpacking begins. Neither Thacker nor Edwards cure this defect.

For at least these additional reasons, claims 8, 20, 12, 23, and 15 are believed to be separately allowable over Lucas, Thacker, and Edwards, either alone or in combination. As such, applicants' representative respectfully requests that these claims be passed to allowance at an early date.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP2193US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Frank J Schumacher IV/
Frank J Schumacher IV
Reg. No. 61,292

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (425) 256-8302
Facsimile (216) 696-8731